UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/496,824	02/02/2000	Ari Juels	SDT-036(7216/51)	6735

23483 7590 02/28/2006

WILMER CUTLER PICKERING HALE AND DORR LLP
60 STATE STREET
BOSTON, MA 02109

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 02/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/496,824	JUELS ET AL.	
	Examiner	Art Unit	
	Syed Zia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 November 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-59* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4,5,8-19,21-30,32,33,36-49 and 51-59* is/are rejected.

7)☒ Claim(s) *3,6,7,20,31,34,35 and 50* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. *2/16-20* .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to arguments filed on November 11, 2005. Original application contained Claims 1-59. Applicant currently amended Claims 13, 41, and 56. The amended filed have been entered and made of record. Presently pending claims are 1-59.

Allowable Subject Matter

Claims 3, 6-7, 20, 31, 34-35, and 50 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Examiner Initiated Interview

In order to simplify the prosecution of this application examiner initiated an interview. This interview was held on Thursday February 19, 2006 and further discussion was done Friday February 17, 2006 and February 20, 2006. During interview examiner pointed out the patentable subject matter to overcome the prior art rejection. Examiner specifically requested to include *client puzzle* and *transactional life cycle of client puzzle*, as described in disclosure, in the independent claims to further distinguish it from challenge/response and authentication/verification protocol of prior arts. Summary of interview is also attached with this office action.

Response to Arguments

Applicant's arguments filed on November 11, 2005 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 1, 18, 27, and 47 applicants argued that Todd (U. S. Patent No. 6,185,689) does not teach or suggest " *computational task, allocating resource for said client if verification is received, and verification of a computational task being performed".*

This is not found persuasive. The system of cited prior arts [Liao et al. (U. S. Patent No. 6,148,405), R.C. Merkle (Communication of the ACM, Volume 21, Number 4, Dated April 1978, 294-299), and Benson U.S. Patent No. 5,935,246] clearly teach system and method of software copy protection system for computer that has challenge mechanism associated with protected item of software, and response *mechanism* in which customer's private keying material is securely stored, using two rounds of authentication by sharing secret encrypt key and challenge-response methods with mutually acceptable cipher where ach authentication process uses a shared secret encrypt hey and challenge/response methods. The server looks for a commonly used cipher and forwards this with a session key to the client.

The software copy protection system includes a challenge mechanism, which is embedded in each protected item of software, and having no access to the customer's private keying material. In operation, the challenge mechanism sends a random challenge to the customer's signature server. The signature server signs the challenge, using the customer's private keying material and then returns the signed challenge to the challenge mechanism. The challenge mechanism then verifies the signed challenge, using the customers public keying material, and prohibits the

customer from using some or all of the protected item of software unless the verification is successful. The mechanism permits every customer to receive an identical copy of the copy-protected program with the embedded challenge mechanism.

As a result, the system of cited prior art does implement and teaches system and method that relates to protecting a server from a communications based denial of service attack.

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that the system of cited prior arts does teach or suggest the subject matter broadly recited in independent Claims 1, 18, 27, and 47and in subsequent dependent Claims. Accordingly, rejections for claims 1,2,4,5,8-19,21-30,32,33,36-49 and 51-59 are respectfully maintained.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

Applicant amended the Claims 13, 41, and 56; therefore, previous rejection under 35 U.S.C. 112, second paragraph, has been withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-10, 14-22, 24-38, 42-53, and 57-59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Liao et al. (U. S. Patent No. 6,148,405) ('Liao hereinafter) in view of R.C. Merkle (Communication of the ACM, Volume 21, Number 4, Dated April 1978, 294-299), and further in view of Benson U.S. Patent No. 5,935,246.

2. With respect to claim 1, Liao teach a method for allocating a resource (abstract), comprising the steps of:

(a) receiving a resource allocation, request from a client (col. 12, line 46 to line 63);

(b) imposing on said client a computational task and a time limit for correct completion of said computational task (col. 7 line 5 to line 25, and col.10 line 22 to line 37);

(d) allocating said resource for said client if the verification is received (col. 12, line 19 to line 25, and col. 12 line 63 to line 66)

While Liao recognize that it is required during a secured communication request for resource to verify a predetermined relationship between a server sent nonce and a received

derivative from the client (col.7 line 17 to line 25). Liao et al. do not explicitly disclose receiving verification that said client has correctly performed computational task within said time limit.

Nonetheless, computational task such as a cryptographic puzzle that is meant to be solved, and controlling the difficulty of puzzle (computational task) complexity is well known, as evidenced by Merkle. In a similar art, Merkle discloses a method creating a puzzle of varying complexity during challenge response communication (page 296 col.1 2nd paragraph to end of col.2) in order to thwart a denial-of-service attack. Given this teaching, a person having ordinary skill in the art would have readily recognized the desirability and advantages of using the challenge-response puzzle authentication protocol to differentiate between legitimate and illegitimate requests in the system taught by Liao, because such a mechanism is a more reliable way to detect bogus requests than the algorithm taught by Liao. Therefore, it would have been obvious to use the challenge-response client puzzle mechanism taught by Merkle to deny the bogus requests described by Liao.

The system of Liao and Merkle discloses forwarding an executable response to the client as part of the challenge-response mechanism. However, the system of Liao and Merkle does not disclose that the executable response is time bound requiring the client to execute the response within a predetermined amount of time. Nonetheless, such a time mechanism is well known, as evidenced by Benson.

In a similar art, Benson discloses methods for preventing unauthorized execution of software using challenge and response, including forwarding an executable response to the client, and receiving the client request with some additional verifiable information if the client request is a valid request (i.e. the client sends a valid response i.e. puzzle response to the server). Benson

further discloses that the executable response is time bound requiring the client to execute the response within a predetermined amount of time ('submit their puzzles within a timeout period). Given this knowledge, a person having ordinary skill in the art would have readily recognized the desirability and advantages of including a executable challenge-response mechanism with a time-based function, as taught by Benson, in the system taught by Liao and Merkle in order to better prevent denial of service attacks (col. 11, lines 19-30). It would' thus have been obvious to include this timeout feature in the system taught by Liao and Merkle to prevent denial-of-service attacks because the implementation of a time limit would limit the amount of time that the client has to complete the required computational task, further increasing the security of the combined system by enabling the server to verify that the task was performed correctly. So long time delays to perform the computational task (client puzzle) would naturally signify that the requests were sent by a "zombie."

3. With respect to claim 18, Liao teach a method for procuring a resource (abstract) comprising the steps of:

(a) communicating a resource allocation request to a server (col. 12, line 46 to line 63);

(b) receiving a computational task from said server, and performing or delegating the performance of said computational task correctly within a known time limit (col. 7 line 5 to line 25, and col.10 line 22 to line 37);

While Liao recognize that it is required during a secured communication request for resource to verify a predetermined relationship between a server sent nonce and a received

derivative from the client (col.7 line 17 to line 25). Liao et al. do not explicitly disclose receiving verification that said client has correctly performed computational task within said time limit.

Nonetheless, computational task such as a cryptographic puzzle that is meant to be solved, and controlling the difficulty of puzzle (computational task) complexity is well known, as evidenced by Merkle. In a similar art, Merkle discloses a method creating a puzzle of varying complexity during challenge response communication (page 296 col.1 2nd paragraph to end of col.2) in order to thwart a denial-of-service attack. Given this teaching, a person having ordinary skill in the art would have readily recognized the desirability and advantages of using the challenge-response puzzle authentication protocol to differentiate between legitimate and illegitimate requests in the system taught by Liao, because such a mechanism is a more reliable way to detect bogus requests than the algorithm taught by Liao. Therefore, it would have been obvious to use the challenge-response client puzzle mechanism taught by Merkle to deny the bogus requests described by Liao.

Although the system of Liao and Merkle discloses forwarding an executable response to the client as part of the challenge-response mechanism. However, the system of Liao and Merkle does not disclose that the executable response is time bound requiring the client to execute the response within a predetermined amount of time. Nonetheless, such a time mechanism is well known, as evidenced by Benson.

In a similar art, Benson discloses methods for preventing unauthorized execution of software using challenge and response, including forwarding an executable response to the client, and receiving the client request with some additional verifiable information if the client request is a valid request (i.e. the client sends a valid response i.e. puzzle response to the server). Benson

further discloses that the executable response is time bound requiring the client to execute the response within a predetermined amount of time ('submit their puzzles within a timeout period). Given this knowledge, a person having ordinary skill in the art would have readily recognized the desirability and advantages of including a executable challenge-response mechanism with a time-based function, as taught by Benson (col. 11, lines 19-30), in the system taught by Liao and Merkle in order to better prevent denial of service attacks. It would' thus have been obvious to include this timeout feature in the system taught by Liao and Merkle to prevent denial-of-service attacks because the implementation of a time limit would limit the amount of time that the client has to complete the required computational task, further increasing the security of the combined system by enabling the server to verify that the task was performed correctly. So long time delays to perform the computational task (client puzzle) would naturally signify that the requests were sent by a "zombie."

4. With respect to claim 27, Liao teach an apparatus for allocating a resource (abstract) comprising:

a first receiver receiving a resource allocation request from a client ((col. 12, line 46 to line 53); a computational task generator for imposing a computational task upon said client for correct performance within a time limit); and a transmitter communicating said computational task to said client ((col. 7 line 5 to line 25, and col.10 line 22 to line 37)); and an allocator allocating said resource for said client (col. 12, line 19 to line 25, and col. 12 line 63 to line 66).

While Liao recognize that it is required during a secured communication request for resource to verify a predetermined relationship between a server sent nonce and a received derivative from the client (col.7 line 17 to line 25). Liao et al. do not explicitly disclose receiving verification that said client has correctly performed computational task within said time limit.

Nonetheless, computational task such as a cryptographic puzzle that is meant to be solved, and controlling the difficulty of puzzle (computational task) complexity is well known, as evidenced by Merkle. In a similar art, Merkle discloses a method creating a puzzle of varying complexity during challenge response communication (page 296 col.1 2nd paragraph to end of col.2) in order to thwart a denial-of-service attack. Given this teaching, a person having ordinary skill in the art would have readily recognized the desirability and advantages of using the challenge-response puzzle authentication protocol to differentiate between legitimate and illegitimate requests in the system taught by Liao, because such a mechanism is a more reliable way to detect bogus requests than the algorithm taught by Liao. Therefore, it would have been obvious to use the challenge-response client puzzle mechanism taught by Merkle to deny the bogus requests described by Liao.

The system of Liao and Merkle discloses forwarding an executable response to the client as part of the challenge-response mechanism. However, the system of Liao and Merkle does not disclose that the executable response is time bound requiring the client to execute the response within a predetermined amount of time. Nonetheless, such a time mechanism is well known, as evidenced by Benson.

In a similar art, Benson discloses methods for preventing unauthorized execution of software using challenge and response, including forwarding an executable response to the client, and

receiving the client request with some additional verifiable information if the client request is a valid request (i.e. the client sends a valid response i.e. puzzle response to the server). Benson further discloses that the executable response is time bound requiring the client to execute the response within a predetermined amount of time ('submit their puzzles within a timeout period). Given this knowledge, a person having ordinary skill in the art would have readily recognized the desirability and advantages of including a executable challenge-response mechanism with a time-based function, as taught by Benson, in the system taught by Liao and Merkle in order to better prevent denial of service attacks (col. 11, lines 19-30). It would' thus have been obvious to include this timeout feature in the system taught by Liao and Merkle to prevent denial-of-service attacks because the implementation of a time limit would limit the amount of time that the client has to complete the required computational task, further increasing the security of the combined system by enabling the server to verify that the task was performed correctly. So long time delays to perform the computational task (client puzzle) would naturally signify that the requests were sent by a "zombie."

5. With respect to claim 47, Liao teach an apparatus for procuring a resource (abstract) comprising:

a first transmitter communicating a resource allocation request to a server (col. 12, line 46 to line 53, and col.3 line 14 to col.4 line 45);

a first receiver receiving a computational task from said server; and a computational task solver correctly performing said computational task within a known time limit (col. 7 line 5 to line 25, and col.10 line 22 to line 37, col.4 line 5 to line 24).

While Liao recognize that it is required during a secured communication request for resource to verify a predetermined relationship between a server sent nonce and a received derivative from the client (col.7 line 17 to line 25). Liao et al. do not explicitly disclose receiving verification that said client has correctly performed computational task within said time limit.

Nonetheless, computational task such as a cryptographic puzzle that is meant to be solved, and controlling the difficulty of puzzle (computational task) complexity is well known, as evidenced by Merkle. In a similar art, Merkle discloses a method creating a puzzle of varying complexity during challenge response communication (page 296 col.1 2nd paragraph to end of col.2) in order to thwart a denial-of-service attack. Given this teaching, a person having ordinary skill in the art would have readily recognized the desirability and advantages of using the challenge-response puzzle authentication protocol to differentiate between legitimate and illegitimate requests in the system taught by Liao, because such a mechanism is a more reliable way to detect bogus requests than the algorithm taught by Liao. Therefore, it would have been obvious to use the challenge-response client puzzle mechanism taught by Merkle to deny the bogus requests described by Liao.

The system of Liao and Merkle discloses forwarding an executable response to the client as part of the challenge-response mechanism. However, the system of Liao and Merkle does not disclose that the executable response is time bound requiring the client to execute the response

within a predetermined amount of time. Nonetheless, such a time mechanism is well known, as evidenced by Benson.

In a similar art, Benson discloses methods for preventing unauthorized execution of software using challenge and response, including forwarding an executable response to the client, and receiving the client request with some additional verifiable information if the client request is a valid request (i.e. the client sends a valid response i.e. puzzle response to the server). Benson further discloses that the executable response is time bound requiring the client to execute the response within a predetermined amount of time ('submit their puzzles within a timeout period). Given this knowledge, a person having ordinary skill in the art would have readily recognized the desirability and advantages of including a executable challenge-response mechanism with a time-based function, as taught by Benson, in the system taught by Liao and Merkle in order to better prevent denial of service attacks (col. 11, lines 19-30). It would' thus have been obvious to include this timeout feature in the system taught by Liao and Merkle to prevent denial-of-service attacks because the implementation of a time limit would limit the amount of time that the client has to complete the required computational task, further increasing the security of the combined system by enabling the server to verify that the task was performed correctly. So long time delays to perform the computational task (client puzzle) would naturally signify that the requests were sent by a "zombie."

6. Claims 2-10, 14-17, 19-22, 24-26, 28-38,42-46, 48-53, and 57-59 are rejected applied as above rejecting claims 1, 18, 27, and 47. Furthermore, the system of Liao, Merkle, and Benson

teaches and describe resource allocation system using a computational task, such as challenge-response puzzle protocol to thwart denial of service attack. Comprising:

7. Claims 2, 19, 29 and 49 are rejected as above in rejecting claim 1, 18, 27, and 47, wherein said resource allocation request comprises a network connection request (Liao: col.3 line 24 to line 27).

9. Claims 4, and 32 rejected as above in rejecting claims 3, and 31, wherein said step (b) comprises communicating the output of a one-way function to said client (Merkle: page 296 col.1 2nd last paragraph)

10. Claims 5, and 33 are rejected as above in rejecting claims 3, and 31, wherein said step (b) comprises communicating the output of a block cipher to said client (Merkle: page 297 col.1 last paragraph to col.2 end of 2nd paragraph).

13. Claims 8, and 36 are rejected as above in rejecting claim 3, and 31,wherein said step (b) comprises communicating a puzzle constructed in a self-authenticating fashion (Liao: col.7 line 5 to line 37, and Merkle: Page 297 3rd paragraph line 1 to line 8).

14. As per claims 9, and 37 the system of Liao and Merkle does not explicitly show a hash image and a partially revealed pre-image to said client. However, Benson teaches communicating a hash image and a partially revealed pre-image to said client (see col. 5, lines 11-40). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Liao and Merkle in view of Benson to use different responses for continuing denial of service attack in the case that attacking system solves the first problem.

15. As per claim 10, and 38, Liao do not explicitly show a receiving and verifying the remaining pre-image. However, Benson teaches receiving the remaining pre-image (Benson: col. 5, lines 11-40). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Liao in view of Benson for the same reasons set forth in claim 9 above.

16. Claim 14, 24, 42, and 57 are rejected as above in rejecting claims 1, 18, 27, and 47 wherein said step (a) comprises receiving a TCP SYN request (Liao col. 6, lines 10-30).

17. Claim 15, 25, 43, and 58 rejected as above in rejecting claims 1, 18, 27, and 47 wherein said step (a) comprises receiving a request to open an SSL connection (Liao: col. 3, lines 15-30).

18. Claims 16, and 44 are rejected as above in rejecting claims 1, and 27, wherein said step (b) comprises the steps of determining if a computational task is to be imposed upon said client based upon the operating circumstances at the time of receiving said resource allocation request from said client; and if a computational task is determined to be imposed upon said client then selecting a computational task responsive to at least one characteristic of said operating circumstances at the time of receiving said resource allocation request; and if a computational task is determined to be imposed upon said client then imposing the selected computational task on said client (col. 7 line 5 to line 25, and col.10 line 22 to line 37, col.4 line 5 to line 24).

19. Claim 17, 26, 45, and 59 are rejected as above in rejecting claims 1, 18, 27, and 47, wherein said step (a) comprises receiving a resource allocation request comprising a query, or accompanied or preceded by a query concerning whether a server is currently imposing computational tasks (Liao: col.7 line 9 to line 25).

20. Claim 20 rejected as above in rejecting claim18, wherein said step (b) comprises receiving said computational task and a time limit for performance of said computational task from said server (Liao: col. 7 line 5 to line 25, col.10 line 22 to line 37, col.4 line 5 to line 24, and Benson: col. 11, lines 19-30).

21. Claim 21, and 52 are rejected as above in rejecting Claim 18, and 47, wherein said step (c) comprises solving a puzzle (Liao: col. 7 line 5 to line 25, col. 12, line 19 to line 66, and col. 12 line 63 to line 66; Merkle: page 296 col.1 2nd paragraph to end of col.2).

22. Claim 22, and 53 are rejected as above in rejecting Claim 18, and 47, wherein said step (c) comprises a linear search of the solution space associated with said computational task (Merkle: page 296 col.2 2nd paragraph).

23. Claim 28 rejected as above in rejecting claim 27, wherein said first receiver and said second receiver comprise the same receiver (Fig.1-2).

24. Claim 30 rejected as above in rejecting claim 27, wherein said transmitter communicates said computational task and a time limit for performance of said computational task to said client (Liao: col. 7 line 5 to line 25, col.10 line 22 to line 37, col.4 line 5 to line 24, and Benson: col. 11, lines 19-30).

25. Claim 46 rejected as above in rejecting claim 27 comprising a time limit generator generating a time limit within which said client must correctly perform said computational task (Liao: col. 7 line 5 to line 25, col.10 line 22 to line 37, col.4 line 5 to line 24, and Benson: col. 11, lines 19-30).

26. Claim 48 rejected as above in rejecting claim 47, wherein said first transmitter and said second transmitter comprise the same transmitter (Fig.1-2).

28. Claim 51 rejected as above in rejecting claim 50 wherein said first receiver and said second receiver comprise the same receiver (Fig.1-2).

29. Claims 11-13, 23, 39-41, and 54-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over the system of Liao, Merkle and Benson and further in view of Ranger U.S. Patent No. 6,301,584.

30. As per claims 11, 23, 39, and 54, the system of Liao, Merkle and Benson teaches the limitation set forth above in claims 3, 18, and 31 to perform a computational task, such as puzzle, to authenticate the client during resource allocation and thwart denial of service attack (Liao: col. 7 line 5 to line 25, col. 12, line 19 to line 66, and col. 12 line 63 to line 66; Merkle: page 296 col.1 2nd paragraph to end of col.2; and Benson: col. 11, lines 19-30), however, the system of Liao, Merkle and Benson does not explicitly disclose wherein said step (b) comprises communicating a plurality of sub-puzzles to a client.

Ranger teaches wherein said step (b) comprises communicating a plurality of sub-puzzles to a client (see col. 20, lines 37-43).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Todd and Benson within the system of Ranger to arrive at the invention as claimed because the references are directed towards a method for allocating a resource, and the implementation of sub-puzzles would improve the ability of the computational task to use different responses for a continuing denial of service attack, during request for resource allocation, in case the attacking system solves a first puzzle, it can be further thwarted by using a new puzzle since the sub-puzzles are constructed independently, thus further increasing the security and increasing the versatility of the combined systems.

31. As per claims 12, 40, and 55 the system of Liao, Merkle and Benson does not explicitly show communicating a plurality of independently constructed sub-puzzles. However, Ranger teaches wherein said step (b) comprises communicating a plurality of independently constructed sub-puzzles (see col. 20, lines 37-43). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Liao, Merkle and Benson, in further view of Ranger for the same reasons set forth in claim 11 above.

32. As per claims 13, 41, and 56 the system of Liao, Merkle and Benson does not explicitly show communicating a plurality of sub-puzzles wherein each sub-puzzle is constructed with some intended overlap. However, Ranger teaches wherein said. step (b) comprises communicating a plurality of sub-puzzles wherein each sub-puzzle is constructed with some intended overlap (see col. 20, lines 37-43). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the system of Liao, Merkle and Benson, in further view of Ranger for the same reasons set forth in claim 11 above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

sz
February 20, 2006